A Fast SHA1 Implementation

ABSTRACT

Provided is an architecture (hardware implementation) for an authentication engine to increase the speed at which SHA1 multi-loop and/or multi-round authentication algorithms may be performed on data packets transmitted over a computer network. As described in this application, the invention has particular application to the variant of the SHA1 authentication algorithms specified by the IPSec cryptography standard. In accordance with the IPSec standard, the invention may be used in conjunction with data encryption/encryption architecture and protocols. However it is also suitable for use in conjunction with other non-IPSec cryptography algorithms, and for applications in which encryption/decryption is not conducted (in IPSec or not) and where it is purely authentication that is accelerated. Among other advantages, an authentication engine in accordance with the present invention provides improved performance with regard to the processing of short data packets.